Ryuk (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 16:22:01 UTC

Ryuk is a ransomware which encrypts its victim's files and asks for a ransom via bitcoin to release the original files. It is has been observed being used to attack companies or professional environments. Cybersecurity experts figured out that Ryuk and Hermes ransomware shares pieces of codes. Hermes is commodity ransomware that has been observed for sale on dark-net forums and used by multiple threat actors.

2024-06-05 · S-RM ·
Exmatter malware levels up: S-RM observes new variant with simultaneous remote code execution and data targeting
BlackCat BlackMatter Conti ExMatter LockBit REvil Ryuk 2023-11-26 · Medium shaddy43 · Shayan Ahmed Khan
From Infection to Encryption: Tracing the Impact of RYUK Ransomware
Ryuk 2023-09-12 · · ANSSI · ANSSI
FIN12: A Cybercriminal Group with Multiple Ransomware
BlackCat Cobalt Strike Conti Hive MimiKatz Nokoyawa Ransomware PLAY Royal Ransom Ryuk SystemBC
2023-07-27 · Bankinfo Security · Mathew J. Schwartz
Are Akira Ransomware's Crypto-Locking Malware Days Numbered?
Akira Ryuk 2022-12-06 · EuRepoC · Camille Borrett, Kerstin Zettl-Schabath, Lena Rottinger
Conti/Wizard Spider
BazarBackdoor Cobalt Strike Conti Emotet IcedID Ryuk TrickBot WIZARD SPIDER 2022-09-13 · AdvIntel · Advanced Intelligence
AdvIntel's State of Emotet aka "SpmTools" Displays Over Million Compromised Machines Through 2022
Conti Cobalt Strike Emotet Ryuk TrickBot 2022-08-31 · Fourcore · Hardik Manocha
Ryuk Ransomware: History, Timeline, And Adversary Simulation
Ryuk 2022-08-22 · Microsoft · Microsoft
Extortion Economics - Ransomware’s new business model
BlackCat Conti Hive REvil AgendaCrypt Black Basta BlackCat Brute Ratel C4 Cobalt Strike Conti Hive Mount Locker Nokoyawa Ransomware REvil Ryuk 2022-05-24 · The Hacker News · Florian Goutin
Malware Analysis: Trickbot
Cobalt Strike Conti Ryuk TrickBot 2022-05-09 · Microsoft · Microsoft 365 Defender Threat Intelligence Team, Microsoft Threat Intelligence Center (MSTIC)
Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself
AnchorDNS BlackCat BlackMatter Conti DarkSide HelloKitty Hive LockBit REvil FAKEUPDATES Griffon ATOMSILO BazarBackdoor BlackCat BlackMatter Blister Cobalt Strike Conti DarkSide Emotet FiveHands Gozi HelloKitty Hive IcedID ISFB JSSLoader LockBit LockFile Maze NightSky Pandora Phobos Phoenix Locker PhotoLoader QakBot REvil Rook Ryuk SystemBC TrickBot WastedLocker BRONZE STARLIGHT 2022-05-05 · Intel 471 · Intel 471
Cybercrime loves company: Conti cooperated with other ransomware gangs

LockBit Maze RagnarLocker Ryuk 2022-04-17 · BushidoToken Blog · BushidoToken

Lessons from the Conti Leaks

BazarBackdoor Conti Emotet IcedID Ryuk TrickBot 2022-04-15 · Arctic Wolf · Arctic Wolf

The Karakurt Web: Threat Intel and Blockchain Analysis Reveals Extension of Conti Business Model

Conti Diavol Ryuk TrickBot 2022-04-13 · Microsoft · Microsoft 365 Defender Threat Intelligence Team

Dismantling ZLoader: How malicious ads led to disabled security tools and ransomware

BlackMatter Cobalt Strike DarkSide Ryuk Zloader 2022-04-13 · Microsoft · Amy Hogan-Burney

Notorious cybercrime gang's botnet disrupted

Ryuk Zloader 2022-04-06 · TRM Labs · TRM Labs

TRM Analysis Corroborates Suspected Ties Between Conti and Ryuk Ransomware Groups and Wizard Spider

Conti Ryuk 2022-03-31 · Trellix · Jambul Tologonov, John Fokker

Conti Leaks: Examining the Panama Papers of Ransomware

LockBit Amadey Buer Conti IcedID LockBit Mailto Maze PhotoLoader Ryuk TrickBot 2022-03-23 · splunk · Shannon Davis

Gone in 52 Seconds…and 42 Minutes: A Comparative Analysis of Ransomware Encryption Speed

Avaddon Babuk BlackMatter Conti DarkSide LockBit Maze Mespinoza REvil Ryuk 2022-03-17 · Sophos · Tilly Travers

The Ransomware Threat Intelligence Center

ATOMSILO Avaddon AvosLocker BlackKingdom Ransomware BlackMatter Conti Cring DarkSide dearcry Dharma Egregor Entropy Epsilon Red Gandcrab Karma LockBit LockFile Mailto Maze Nefilim RagnarLocker Ragnarok REvil RobinHood Ryuk SamSam Snatch WannaCryptor WastedLocker 2022-03-02 · · elDiario · Carlos del Castillo

Cybercrime bosses warn that they will "fight back" if Russia is hacked

Conti Ryuk 2022-03-02 · KrebsOnSecurity · Brian Krebs

Conti Ransomware Group Diaries, Part II: The Office

Conti Emotet Ryuk TrickBot 2022-02-23 · splunk · Shannon Davis, SURGe

An Empirically Comparative Analysis of Ransomware Binaries

Avaddon Babuk BlackMatter Conti DarkSide LockBit Maze Mespinoza REvil Ryuk 2022-01-19 · Blackberry · The BlackBerry Research & Intelligence Team

Kraken the Code on Prometheus

Prometheus Backdoor BlackMatter Cerber Cobalt Strike DCRat Ficker Stealer QakBot REvil Ryuk 2021-11-18 · Medium 0xchina · Hamad Alnakal

Malware reverse engineering (Ryuk Ransomware)

Ryuk 2021-10-22 · HUNT & HACKETT · Krijn de Mik

Advanced IP Scanner: the preferred scanner in the A(P)T toolbox

Conti DarkSide Dharma Egregor Hades REvil Ryuk 2021-10-07 · Mandiant · Adam Brunner, Genevieve Stark, Jennifer Brooks, Jeremy Kennelly, Joshua Shilko, Kimberly Goody, Zach Riddle

FIN12: The Prolific Ransomware Intrusion Threat Actor That Has Aggressively Pursued Healthcare Targets

BazarBackdoor GRIMAGENT Ryuk 2021-10-05 · Trend Micro · Byron Gelera, Fyodor Yarochkin, Janus Agcaoili, Nikko Tamana

Ransomware as a Service: Enabler of Widespread Attacks

Cerber Conti DarkSide Gandcrab Locky Nefilim REvil Ryuk 2021-09-16 · RiskIQ · RiskIQ

Untangling the Spider Web: The Curious Connection Between WIZARD SPIDER’s Ransomware Infrastructure and a Windows Zero-Day Exploit

Cobalt Strike Ryuk 2021-08-15 · Symantec · Threat Hunter Team

The Ransomware Threat

Babuk BlackMatter DarkSide Avaddon Babuk BADHATCH BazarBackdoor BlackMatter Clop Cobalt Strike Conti DarkSide DoppelPaymer Egregor Emotet FiveHands FriedEx Hades IcedID LockBit Maze MegaCortex MimiKatz QakBot RagnarLocker REvil Ryuk TrickBot WastedLocker 2021-08-05 · KrebsOnSecurity · Brian Krebs

Ransomware Gangs and the Name Game Distraction

DarkSide RansomEXX Babuk Cerber Conti DarkSide DoppelPaymer Egregor FriedEx Gandcrab Hermes Maze RansomEXX REvil Ryuk Sekhmet 2021-07-07 · McAfee · McAfee Labs

Ryuk Ransomware Now Targeting Webservers

Cobalt Strike Ryuk 2021-06-16 · Proofpoint · Daniel Blackford, Garrett M. Graff, Selena Larson

The First Step: Initial Access Leads to Ransomware

BazarBackdoor Egregor IcedID Maze QakBot REvil Ryuk TrickBot WastedLocker TA570 TA575 TA577 2021-06-09 · Twitter (@SecurityJoes) · SecurityJoes

Tweet on .NET builder of a Ryuk imposter malware

Ryuk 2021-06-07 · Medium walmartglobaltech · Jason Reaves, Joshua Platt

Inside the SystemBC Malware-As-A-Service

Ryuk SystemBC TrickBot 2021-05-22 · Youtube (ACPEnw) · YouTube (ACPEnw)

Lessons Learned from a Cyber Attack System Admin Perspective

Ryuk 2021-05-18 · The Record · Catalin Cimpanu

Darkside gang estimated to have made over $90 million from ransomware attacks

DarkSide DarkSide Mailto Maze REvil Ryuk 2021-05-18 · Bleeping Computer · Ionut Ilascu

DarkSide ransomware made $90 million in just nine months

DarkSide DarkSide Egregor Gandcrab Mailto Maze REvil Ryuk 2021-05-06 · Cyborg Security · Brandon Denker

Ransomware: Hunting for Inhibiting System Backup or Recovery

Avaddon Conti DarkSide LockBit Mailto Maze Mespinoza Nemty PwndLocker RagnarLocker RansomEXX REvil Ryuk Snatch ThunderX 2021-05-06 · Sophos Labs · Bill Kearney, Kyle Link, Matthew Sharf, Peter Mackenzie, Tilly Travers

MTR in Real Time: Pirates pave way for Ryuk ransomware

Ryuk 2021-04-26 · CoveWare · CoveWare

Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

Avaddon Clop Conti DarkSide Egregor LockBit Mailto Phobos REvil Ryuk SunCrypt 2021-04-17 · Advanced Intelligence · Al Calleo, Vitali Kremez, Yelisey Boguslavskiy

Adversary Dossier: Ryuk Ransomware Anatomy of an Attack in 2021

Ryuk 2021-04-07 · ANALYST1 · Jon DiMaggio

Ransom Mafia Analysis of the World's First Ransomware Cartel

Conti Egregor LockBit Maze RagnarLocker Ryuk SunCrypt TA2101 VIKING SPIDER 2021-03-21 · Blackberry · Blackberry Research

2021 Threat Report

Bashlite FritzFrog IPStorm Mirai Tsunami elf.wellmess AppleJeus Dacls EvilQuest Manuscrypt Astaroth BazarBackdoor Cerber Cobalt Strike Emotet FinFisher RAT Kwampirs MimiKatz NjRAT Ryuk SmokeLoader

TrickBot 2021-03-17 · Palo Alto Networks Unit 42 · Unit42

Ransomware Threat Report 2021

RansomEXX Dharma DoppelPaymer Gandcrab Mailto Maze Phobos RansomEXX REvil Ryuk WastedLocker

2021-03-04 · NCC Group · Ollie Whitehouse

Deception Engineering: exploring the use of Windows Service Canaries against ransomware

Ryuk 2021-03-01 · YouTube (Malware_Analyzing_&_RE_Tips_Tricks) · Jiří Vinopal

Ryuk Ransomware - Advanced using of Scylla for Imports reconstruction

Ryuk 2021-03-01 · · CCN-CERT · CCN-CERT

Informe Código DañinoCCN-CERT ID-03/21: RyukRansomware

Ryuk 2021-03-01 · Group-IB · Oleg Skulkin, Roman Rezvukhin, Semyon Rogachev

Ransomware Uncovered 2020/2021

RansomEXX BazarBackdoor Buer Clop Conti DoppelPaymer Dridex Egregor IcedID Maze PwndLocker QakBot

RansomEXX REvil Ryuk SDBbot TrickBot Zloader 2021-02-28 · PWC UK · PWC UK

Cyber Threats 2020: A Year in Retrospect

elf.wellmess FlowerPower PowGoop 8.t Dropper Agent.BTZ Agent Tesla Appleseed Ave Maria Bankshot

BazarBackdoor BLINDINGCAN Chinoxy Conti Cotx RAT Crimson RAT DUSTMAN Emotet FriedEx

FunnyDream Hakbit Mailto Maze METALJACK Nefilim Oblique RAT Pay2Key PlugX QakBot REvil Ryuk

StoneDrill StrongPity SUNBURST SUPERNOVA TrickBot TurlaRPC Turla SilentMoon WastedLocker WellMess

Winnti ZeroCleare APT10 APT23 APT27 APT31 APT41 BlackTech BRONZE EDGEWOOD Inception

Framework MUSTANG PANDA Red Charon Red Nue Sea Turtle Tonto Team 2021-02-27 · 4rchibld · 4rchibld

Nice to meet you, too. My name is Ryuk.

Ryuk 2021-02-25 · ANSSI · CERT-FR

Ryuk Ransomware

BazarBackdoor Buer Conti Emotet Ryuk TrickBot 2021-02-23 · CrowdStrike · CrowdStrike

2021 Global Threat Report

RansomEXX Amadey Anchor Avaddon BazarBackdoor Clop Cobalt Strike Conti Cutwail DanaBot DarkSide

DoppelPaymer Dridex Egregor Emotet Hakbit IcedID JSOutProx KerrDown LockBit Mailto Maze MedusaLocker

Mespinoza Mount Locker NedDnLoader Nemty Pay2Key PlugX Pushdo PwndLocker PyXie QakBot Quasar RAT

RagnarLocker Ragnarok RansomEXX REvil Ryuk Sekhmet ShadowPad SmokeLoader Snake SUNBURST

SunCrypt TEARDROP TrickBot WastedLocker Winnti Zloader Evilnum OUTLAW SPIDER RIDDLE SPIDER

SOLAR SPIDER VIKING SPIDER 2021-02-22 · YouTube (Malware_Analyzing_&_RE_Tips_Tricks) · Jiří Vinopal

Ryuk Ransomware API Resolving in 10 minutes

Ryuk 2021-02-16 · Proofpoint · Proofpoint Threat Research Team

Q4 2020 Threat Report: A Quarterly Analysis of Cybersecurity Trends, Tactics and Themes

Emotet Ryuk NARWHAL SPIDER TA800 2021-02-11 · CTI LEAGUE · CTI LEAGUE

CTIL Darknet Report – 2021

Conti Mailto Maze REvil Ryuk 2021-02-04 · ClearSky · ClearSky Research Team

CONTI Modus Operandi and Bitcoin Tracking

Conti Ryuk 2021-02-02 · · CRONUP · Germán Fernández

De ataque con Malware a incidente de Ransomware

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DanaBot Dharma Dridex Egregor Emotet Empire

Downloader FriedEx GootKit IcedID MegaCortex Nemty Phorpiex PwndLocker PyXie QakBot RansomEXX

REvil Ryuk SDBbot SmokeLoader TrickBot Zloader 2021-02-01 · Twitter (@IntelAdvanced) · Advanced Intelligence

Tweet on Active Directory Exploitation by RYUK "one" group

Ryuk 2021-01-31 · The DFIR Report · The DFIR Report

Bazar, No Ryuk?

BazarBackdoor Cobalt Strike Ryuk 2021-01-28 · Huntress Labs · John Hammond

Analyzing Ryuk Another Link in the Cyber Attack Chain

BazarBackdoor Ryuk 2021-01-25 · Twitter (@IntelAdvanced) · Advanced Intelligence

Tweet on Ryuk Ransomware group's post exploitation tactics including usage of Keethief tool

Ryuk 2021-01-07 · Advanced Intelligence · Brian Carter, HYAS, Vitali Kremez

Crime Laundering Primer: Inside Ryuk Crime (Crypto) Ledger & Risky Asian Crypto Traders

Ryuk 2020-12-28 · 0xC0DECAFE · Thomas Barabosch

Never upload ransomware samples to the Internet

Ryuk 2020-12-22 · TRUESEC · Mattias Wåhlén

Collaboration between FIN7 and the RYUK group, a Truesec Investigation

Carbanak Cobalt Strike Ryuk 2020-12-21 · IronNet · Adam Hlavek, Kimberly Ortiz

Russian cyber attack campaigns and actors

WellMail elf.wellmess Agent.BTZ BlackEnergy EternalPetya Havex RAT Industroyer Ryuk Triton WellMess 2020-12-16 · Accenture · Paul Mansfield

Tracking and combatting an evolving danger: Ransomware extortion

DarkSide Egregor Maze Nefilim RagnarLocker REvil Ryuk SunCrypt 2020-12-10 · US-CERT · FBI, MS-ISAC, US-CERT

Alert (AA20-345A): Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data

PerlBot Shlayer Agent Tesla Cerber Dridex Ghost RAT Kovter Maze MedusaLocker Nanocore RAT Nefilim REvil Ryuk Zeus 2020-12-10 · CyberInt · CyberInt

Ryuk Crypto-Ransomware

Ryuk TrickBot 2020-12-10 · Cybereason · Joakim Kandefelt

Cybereason vs. Ryuk Ransomware

BazarBackdoor Ryuk TrickBot 2020-12-09 · Cisco · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends from Fall 2020

Cobalt Strike IcedID Maze RansomEXX Ryuk 2020-11-20 · ZDNet · Catalin Cimpanu

The malware that usually installs ransomware and you need to remove right away

Avaddon BazarBackdoor Buer Clop Cobalt Strike Conti DoppelPaymer Dridex Egregor Emotet FriedEx MegaCortex Phorpiex PwndLocker QakBot Ryuk SDBbot TrickBot Zloader 2020-11-19 · Threatpost · Elizabeth Montalbano

APT Exploits Microsoft Zerologon Bug: Targets Japanese Companies

Quasar RAT Ryuk 2020-11-18 · DomainTools · Joe Slowik

Analyzing Network Infrastructure as Composite Objects

Ryuk 2020-11-16 · Intel 471 · Intel 471

Ransomware-as-a-service: The pandemic within a pandemic

Avaddon Clop Conti DoppelPaymer Egregor Hakbit Mailto Maze Mespinoza RagnarLocker REvil Ryuk SunCrypt ThunderX 2020-11-14 · Medium 0xastrovax · astrovax

Deep Dive Into Ryuk Ransomware

Hermes Ryuk 2020-11-06 · Advanced Intelligence · Vitali Kremez

Anatomy of Attack: Inside BazarBackdoor to Ryuk Ransomware "one" Group via Cobalt Strike

BazarBackdoor Cobalt Strike Ryuk 2020-11-05 · The DFIR Report · The DFIR Report

Ryuk Speed Run, 2 Hours to Ransom

BazarBackdoor Cobalt Strike Ryuk 2020-11-05 · SCYTHE · Jorge Orchilles, Sean Lyngaas

#ThreatThursday - Ryuk

BazarBackdoor Ryuk 2020-11-05 · Twitter (@ffforward) · TheAnalyst

Tweet on Zloader infection leads to Cobaltstrike Installation and deployment of RYUK

Cobalt Strike Ryuk Zloader 2020-11-05 · Github (scythe-io) · SCYTHE

Ryuk Adversary Emulation Plan

Ryuk 2020-11-04 · VMRay · Giovanni Vigna

Trick or Threat: Ryuk ransomware targets the health care industry

BazarBackdoor Cobalt Strike Ryuk TrickBot 2020-10-31 · splunk · Ryan Kovar

Ryuk and Splunk Detections

Ryuk 2020-10-30 · Cofense · The Cofense Intelligence Team

The Ryuk Threat: Why BazarBackdoor Matters Most

BazarBackdoor Ryuk 2020-10-30 · Github (ThreatConnect-Inc) · ThreatConnect

UNC 1878 Indicators from Threatconnect

BazarBackdoor Cobalt Strike Ryuk 2020-10-29 · Reuters · Christopher Bing, Joseph Menn

Building wave of ransomware attacks strike U.S. hospitals

Ryuk 2020-10-29 · Bleeping Computer · Lawrence Abrams

Hacking group is targeting US hospitals with Ryuk ransomware

Ryuk 2020-10-29 · CNN · Alex Marquardt, Lauren Mascarenhas, Vivian Salama

Several hospitals targeted in new wave of ransomware attacks

Ryuk 2020-10-29 · McAfee · McAfee Labs

McAfee Labs Threat Advisory Ransom-Ryuk

Ryuk 2020-10-29 · Palo Alto Networks Unit 42 · Brad Duncan, Brittany Barbehenn, Doel Santos

Threat Assessment: Ryuk Ransomware and Trickbot Targeting U.S. Healthcare and Public Health Sector

Anchor BazarBackdoor Ryuk TrickBot 2020-10-29 · Red Canary · The Red Canary Team

A Bazar start: How one hospital thwarted a Ryuk ransomware outbreak

Cobalt Strike Ryuk TrickBot 2020-10-29 · Twitter (@SophosLabs) · SophosLabs

Tweet on similarities between BUER in-memory loader & RYUK in-memory loader

Buer Ryuk 2020-10-29 · RiskIQ · RiskIQ

Ryuk Ransomware: Extensive Attack Infrastructure Revealed

Cobalt Strike Ryuk 2020-10-29 · Twitter (@anthomsec) · Andrew Thompson

Tweet on UNC1878 activity

BazarBackdoor Ryuk TrickBot UNC1878 2020-10-28 · FireEye · Douglas Bienstock, Jeremy Kennelly, Joshua Shilko, Kimberly Goody, Steve Elovitz

Unhappy Hour Special: KEGTAP and SINGLEMALT With a Ransomware Chaser

BazarBackdoor Cobalt Strike Ryuk UNC1878 2020-10-28 · SophosLabs Uncut · Anand Ajjan, Bill Kearny, Brett Cove, Elida Leite, Gabor Szappanos, Peter Mackenzie, Sean Gallagher, Syed Shahram

Hacks for sale: inside the Buer Loader malware-as-a-service

Buer Ryuk Zloader 2020-10-28 · CISA · CISA, FBI, HHS

AA20-302A: Ransomware Activity Targeting the Healthcare and Public Health Sector

AnchorDNS Anchor BazarBackdoor Ryuk 2020-10-28 · KrebsOnSecurity · Brian Krebs

FBI, DHS, HHS Warn of Imminent, Credible Ransomware Threat Against U.S. Hospitals

Ryuk 2020-10-28 · Youtube (SANS Digital Forensics and Incident Response) · Aaron Stephens, Katie Nickels, Van Ta

STAR Webcast: Spooky RYUKy: The Return of UNC1878

Ryuk 2020-10-28 · Github (aaronst) · Aaron Stephens

UNC1878 indicators

Ryuk UNC1878 2020-10-28 · Youtube (SANS Institute) · Aaron Stephens, Katie Nickels, Van Ta

Spooky RYUKy: The Return of UNC1878 | SANS STAR Webcast

Ryuk UNC1878 2020-10-27 · Bleeping Computer · Lawrence Abrams

Steelcase furniture giant hit by Ryuk ransomware attack

Ryuk 2020-10-26 · ThreatConnect · ThreatConnect Research Team

ThreatConnect Research Roundup: Ryuk and Domains Spoofing ESET and Microsoft

Ryuk 2020-10-22 · Sentinel LABS · Marco Figueroa

An Inside Look at How Ryuk Evolved Its Encryption and Evasion Techniques

Ryuk 2020-10-22 · Bleeping Computer · Lawrence Abrams

French IT giant Sopra Steria hit by Ryuk ransomware

Ryuk 2020-10-20 · · Bundesamt für Sicherheit in der Informationstechnik · BSI

Die Lage der IT-Sicherheit in Deutschland 2020

Clop Emotet REvil Ryuk TrickBot 2020-10-18 · The DFIR Report · The DFIR Report

Ryuk in 5 Hours

BazarBackdoor Cobalt Strike Ryuk 2020-10-16 · CrowdStrike · The Crowdstrike Intel Team

WIZARD SPIDER Update: Resilient, Reactive and Resolute

BazarBackdoor Conti Ryuk TrickBot 2020-10-16 · ThreatConnect · ThreatConnect Research Team

ThreatConnect Research Roundup: Possible Ryuk Infrastructure

Ryuk 2020-10-14 · Sophos · Sean Gallagher

They’re back: inside a new Ryuk ransomware attack

Cobalt Strike Ryuk SystemBC 2020-10-13 · VirusTotal · Gerardo Fernández, Vicente Diaz

Tracing fresh Ryuk campaigns itw

Ryuk 2020-10-12 · Microsoft · Tom Burt

New action to combat ransomware ahead of U.S. elections

Ryuk TrickBot 2020-10-12 · Symantec · Threat Hunter Team

Trickbot: U.S. Court Order Hits Botnet’s Infrastructure

Ryuk TrickBot 2020-10-12 · Advanced Intelligence · Roman Marshanski, Vitali Kremez

"Front Door" into BazarBackdoor: Stealthy Cybercrime Weapon

BazarBackdoor Cobalt Strike Ryuk 2020-10-08 · The DFIR Report · The DFIR Report

Ryuk’s Return

BazarBackdoor Cobalt Strike Ryuk 2020-10-02 · Health Sector Cybersecurity Coordination Center (HC3) · Health Sector Cybersecurity Coordination Center (HC3)

Report 202010021600: Recent Bazarloader Use in Ransomware Campaigns

BazarBackdoor Cobalt Strike Ryuk TrickBot 2020-10-01 · KELA · Victoria Kivilevich

To Attack or Not to Attack: Targeting the Healthcare Sector in the Underground Ecosystem

Conti DoppelPaymer Mailto Maze REvil Ryuk SunCrypt 2020-09-29 · PWC UK · Andy Auld

What's behind the increase in ransomware attacks this year?

DarkSide Avaddon Clop Conti DoppelPaymer Dridex Emotet FriedEx Mailto PwndLocker QakBot REvil Ryuk SMAUG SunCrypt TrickBot WastedLocker 2020-09-24 · Kaspersky Labs · Kaspersky Lab ICS CERT

Threat landscape for industrial automation systems - H1 2020

Poet RAT Mailto Milum RagnarLocker REvil Ryuk Snake 2020-09-01 · Cisco Talos · Caitlin Huey, David Liebenberg

Quarterly Report: Incident Response trends in Summer 2020

Cobalt Strike LockBit Mailto Maze Ryuk 2020-08-20 · sensecy · cyberthreatinsider

Global Ransomware Attacks in 2020: The Top 4 Vulnerabilities

Clop Maze REvil Ryuk 2020-08-18 · Arete · Arete Incident Response

Is Conti the New Ryuk?

Conti Ryuk 2020-08-01 · Temple University · CARE

Critical Infrastructure Ransomware Attacks

CryptoLocker Cryptowall DoppelPaymer FriedEx Mailto Maze REvil Ryuk SamSam WannaCryptor 2020-06-23 · Bleeping Computer · Ionut Ilascu

Ryuk ransomware deployed two weeks after Trickbot infection

Ryuk 2020-06-15 · Cisco Talos · Caitlin Huey, David Liebenberg

Quarterly report: Incident Response trends in Summer 2020

Ryuk 2020-05-05 · N1ght-W0lf Blog · Abdallah Elshinbary

Deep Analysis of Ryuk Ransomware

Ryuk 2020-04-19 · SecurityLiterate · Kyle Cucci

Reversing Ryuk: A Technical Analysis of Ryuk Ransomware

Ryuk 2020-04-14 · Intel 471 · Intel 471

Understanding the relationship between Emotet, Ryuk and TrickBot

Emotet Ryuk TrickBot 2020-03-31 · FireEye · Aaron Stephens, Van Ta

It’s Your Money and They Want It Now - The Cycle of Adversary Pursuit

Ryuk TrickBot UNC1878 2020-03-25 · Wilbur Security · JW

Trickbot to Ryuk in Two Hours

Cobalt Strike Ryuk TrickBot 2020-03-05 · Microsoft · Microsoft Threat Protection Intelligence Team

Human-operated ransomware attacks: A preventable disaster

Dharma DoppelPaymer Dridex EternalPetya Gandcrab Hermes LockerGoga MegaCortex MimiKatz REvil RobinHood Ryuk SamSam TrickBot WannaCryptor PARINACOTA 2020-03-04 · Bleeping Computer · Lawrence Abrams

Ryuk Ransomware Attacked Epiq Global Via TrickBot Infection

Ryuk TrickBot 2020-03-04 · CrowdStrike · CrowdStrike

2020 CrowdStrike Global Threat Report

MESSAGETAP More_eggs 8.t Dropper Anchor BabyShark BadNews Clop Cobalt Strike CobInt Cobra Carbon System Cutwail DanaBot Dharma DoppelDridex DoppelPaymer Dridex Emotet FlawedAmmyy FriedEx Gandcrab Get2 IcedID ISFB KerrDown LightNeuron LockerGoga Maze MECHANICAL Necurs Nokki Outlook Backdoor Phobos Predator The Thief QakBot REvil RobinHood Ryuk SDBbot Skipper SmokeLoader TerraRecon TerraStealer TerraTV TinyLoader TrickBot Vidar Winnti ANTHROPOID SPIDER APT23 APT31 APT39 APT40 BlackTech BuhTrap Charming Kitten CLOCKWORK SPIDER DOPPEL SPIDER FIN7 Gamaredon Group

GOBLIN PANDA MONTY SPIDER MUSTANG PANDA NARWHAL SPIDER NOCTURNAL SPIDER PINCHY SPIDER SALTY SPIDER SCULLY SPIDER SMOKY SPIDER Thrip VENOM SPIDER VICEROY TIGER 2020-03-03 · PWC UK · PWC UK

Cyber Threats 2019:A Year in Retrospect

KevDroid MESSAGETAP magecart AndroMut Cobalt Strike CobInt Crimson RAT DNSpionage Dridex Dtrack Emotet FlawedAmmyy FlawedGrace FriedEx Gandcrab Get2 GlobeImposter Grateful POS ISFB Kazuar LockerGoga Nokki QakBot Ramnit REvil Rifdoor RokRAT Ryuk shadowhammer ShadowPad Shifu Skipper StoneDrill Stuxnet TrickBot Winnti ZeroCleare APT41 MUSTANG PANDA Sea Turtle 2020-03-02 · · c't · Christian Wölbert

Was Emotet anrichtet – und welche Lehren die Opfer daraus ziehen

Emotet Ryuk 2020-02-25 · RSA Conference · Joel DeCapua

Feds Fighting Ransomware: How the FBI Investigates and How You Can Help

FastCash Cerber Defray Dharma FriedEx Gandcrab GlobeImposter Mamba Phobos Rapid Ransom REvil Ryuk SamSam Zeus 2020-02-13 · Quick Heal · Goutam Tripathy

A Deep Dive Into Wakeup On Lan (WoL) Implementation of Ryuk

Ryuk 2020-02-12 · VMWare Carbon Black · AC, Rachel E. King

Ryuk Ransomware Technical Analysis

Ryuk 2020-02-10 · Malwarebytes · Adam Kujawa, Chris Boyd, David Ruiz, Jérôme Segura, Jovi Umawing, Nathan Collier, Pieter Arntz, Thomas Reed, Wendy Zamora

2020 State of Malware Report

magecart Emotet QakBot REvil Ryuk TrickBot WannaCryptor 2020-01-29 · ANSSI · ANSSI

État de la menace rançongiciel

Clop Dharma FriedEx Gandcrab LockerGoga Maze MegaCortex REvil RobinHood Ryuk SamSam 2020-01-29 · ZDNet · Catalin Cimpanu

DOD contractor suffers ransomware infection

Ryuk 2020-01-24 · ReversingLabs · Robert Simmons

Hunting for Ransomware

Ryuk 2020-01-24 · Bleeping Computer · Lawrence Abrams

New Ryuk Info Stealer Targets Government and Military Secrets

Ryuk 2020-01-17 · Secureworks · Keita Yamazaki, Tamada Kiyotaka, You Nakatsuru

Is It Wrong to Try to Find APT Techniques in Ransomware Attack?

Defray Dharma FriedEx Gandcrab GlobeImposter Matrix Ransom MedusaLocker Phobos REvil Ryuk SamSam Scarab Ransomware 2020-01-14 · Bleeping Computer · Lawrence Abrams

Ryuk Ransomware Uses Wake-on-Lan To Encrypt Offline Devices

Ryuk 2020-01-01 · Secureworks · SecureWorks

GOLD ULRICK

Empire Downloader Ryuk TrickBot WIZARD SPIDER 2020-01-01 · Blackberry · Blackberry Research

State of Ransomware

Maze MedusaLocker Nefilim Phobos REvil Ryuk STOP 2019-12-26 · Bleeping Computer · Lawrence Abrams

Ryuk Ransomware Stops Encrypting Linux Folders

Ryuk 2019-12-21 · Decrypt · Adriana Hamacher

How ransomware exploded in the age of Bitcoin

Ryuk 2019-12-19 · Malwarebytes · Jovi Umawing

Threat spotlight: the curious case of Ryuk ransomware

Ryuk 2019-12-15 · Bleeping Computer · Lawrence Abrams

Ryuk Ransomware Likely Behind New Orleans Cyberattack

Ryuk 2019-12-09 · Emsisoft · EmsiSoft Malware Lab

Caution! Ryuk Ransomware decryptor damages larger files, even if you pay

Ryuk 2019-11-27 · Twitter (@Prosegur) · Prosegur

Tweet on Incident of Information Security

Ryuk 2019-11-06 · · Heise Security · Thomas Hungenberg

Emotet, Trickbot, Ryuk – ein explosiver Malware-Cocktail

Emotet Ryuk TrickBot 2019-11-05 · Information Age · David Braue

Hospital cyberattack could have been avoided

Ryuk 2019-11-01 · · CCN-CERT · CCN-CERT

Informe Código Dañino CCN-CERT ID-26/19

Ryuk 2019-11-01 · CrowdStrike · Alexander Hanel, Brett Stone-Gross

WIZARD SPIDER Adds New Features to Ryuk for Targeting Hosts on LAN

Ryuk WIZARD SPIDER 2019-05-09 · GovCERT.ch · GovCERT.ch

Severe Ransomware Attacks Against Swiss SMEs

Emotet LockerGoga Ryuk TrickBot 2019-04-05 · FireEye · Alex Pennino, Andrew Thompson, Ben Fedore, Brendan McKeague, Douglas Bienstock, Geoff Ackerman, Van Ta

Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware

LockerGoga Ryuk FIN6 2019-04-02 · Cybereason · Lior Rochberger, Matan Zatz, Noa Pinkas

Triple Threat: Emotet Deploys Trickbot to Steal Data & Spread Ryuk

Ryuk TrickBot 2019-03-26 · · ANSSI · ANSSI

INFORMATIONS CONCERNANTLES RANÇONGICIELSLOCKERGOGA ET RYUK

Ryuk 2019-03-26 · · ANSSI · ANSSI

INFORMATION REGARDING LOCKERGOGA AND RYUK RANSOMWARE - NEW ATTACK CAMPAIGN AND TECHNICAL INDICATORS

LockerGoga Ryuk 2019-01-11 · FireEye · Christopher Glyer, Jaideep Natu, Jeremy Kennelly, Kimberly Goody

A Nasty Trick: From Credential Theft Malware to Business Disruption

Ryuk TrickBot GRIM SPIDER WIZARD SPIDER 2019-01-10 · CrowdStrike · Alexander Hanel

Big Game Hunting with Ryuk: Another Lucrative Targeted Ransomware

Ryuk GRIM SPIDER MUMMY SPIDER STARDUST CHOLLIMA WIZARD SPIDER 2019-01-09 · McAfee · Christiaan Beek, John Fokker

Ryuk Ransomware Attack: Rush to Attribution Misses the Point

Ryuk 2019-01-01 · Virus Bulletin · Gabriela Nicolao, Luciano Martins

Shinigami's Revenge: The Long Tail of Ryuk Malware

Ryuk 2018-12-29 · Los Angeles Times · Emily Alpert Reyes, Meg James, Tony Barboza

Malware attack disrupts delivery of L.A. Times and Tribune papers across the U.S.

Ryuk 2018-08-20 · Check Point · Ben Herzog, Itay Cohen

Ryuk Ransomware: A Targeted Campaign Break-Down

Ryuk

▶ [TLP:WHITE] win_ryuk_auto (20251219 | Detects win.ryuk.)
